

Документ подписан простой электронной подписью
 Информация о владельце:
 ФИО: Петренко Вячеслав Иванович
 Должность: и.о. директора Института цифрового развития
 Дата подписания: 05.07.2024 09:35:26
 Уникальный программный ключ:
 b47f96eea65a20e275f94bbf7b0b10000e7ad4d

Аннотация дисциплины

Наименование дисциплины	Оценка защищенности компьютерных систем и сетей
Содержание	Анализ проблемы информационной безопасности предприятия. Стандарты информационной безопасности. Политики безопасности. Методы качественной оценки систем информационной безопасности. Оценка уровня информационной безопасности. Оценка рисков. Тестирование систем информационной безопасности. Методы количественной оценки систем информационной безопасности. Метод экспертных оценок. Метод информационных потоков. Графовый метод. Метод весовых коэффициентов. Методы и средства сбора предварительной информации об анализируемой сети. Предварительный сбор информации о домене. Идентификация узлов и портов сетевых служб. Методы и средства идентификации служб и приложений в анализируемой сети. Идентификации служб и приложений для открытых портов. Методы и средства идентификации ОС в анализируемой сети. Анализ возможностей сетевых сканеров. Методы и средства идентификации уязвимостей анализируемой сети по косвенным признакам. Сетевые службы DNS, HTTP, SSH. Методы и средства идентификации уязвимостей анализируемой сети на основе тестов. Сканеры безопасности. Методы и средства идентификации уязвимостей веб приложений. Поиск уязвимостей веб-приложений. Методы и средства идентификации уязвимостей корпоративной сети. Профиль сканирования уязвимостей. Сбор информации о веб-приложении. Тестирование защищенности транспортного уровня. Тестирование защищенности механизма управления доступом. Тестирование защищенности механизма управления сессиями. Тестирование на устойчивость к атакам отказа в обслуживании. Поиск уязвимостей к атакам CSRF. Поиск уязвимостей к атакам XSS. Поиск уязвимостей к атакам SQL-injection. Поиска уязвимостей к атакам RCE. Сканирование уязвимостей веб-приложений.
Реализуемые компетенции	ПК-1. Способен разрабатывать требования по защите информации для формирования политик безопасности компьютерных систем и сетей. ПК-2. Способен проводить анализ безопасности компьютерных систем. ПК-3. Способен проводить сертификацию программно-аппаратных средств защиты информации и анализ результатов.
Результаты освоения дисциплины (модуля)	ПК-1 Знать: принципы построения компьютерных систем и сетей; модели безопасности компьютерных систем; виды политик безопасности компьютерных систем и сетей; принципы построения средств криптографической защиты информации; национальные, межгосударственные и международные стандарты в области защиты информации; возможности используемых и планируемых к использованию средств защиты информации; нормативные правовые акты в области защиты информации; руководящие и методические документы уполномоченных

	федеральных органов исполнительной власти по защите информации; организационные меры по защите информации Уметь: анализировать компьютерную систему с целью определения необходимого уровня защищенности и доверия; разрабатывать профили защиты компьютерных систем; формулировать задания по безопасности компьютерных систем; выполнять анализ безопасности компьютерных систем и разрабатывать рекомендации по эксплуатации системы защиты информации. Владеть: навыками разработки технических заданий на создание средств защиты информации; классификации информационной системы по требованиям защиты информации. ПК-2 Знать: уязвимости компьютерных систем и сетей; криптографические методы защиты информации; принципы построения систем управления базами данных; средства анализа конфигураций; национальные, межгосударственные и международные стандарты в области защиты информации; нормативные правовые акты в области защиты информации; руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации; организационные меры по защите информации. Уметь: анализировать компьютерную систему с целью определения уровня защищенности и доверия; прогнозировать возможные пути развития действий нарушителя информационной безопасности; производить анализ политики безопасности на предмет адекватности; проводить мониторинг, анализ и сравнение эффективности программно-аппаратных средств защиты информации в операционных системах; составлять и оформлять аналитический отчет по результатам проведенного анализа; разрабатывать предложения по устранению выявленных уязвимостей. Владеть: навыками определения уровня защищенности и доверия в компьютерных системах; оценки рисков, связанных с осуществлением угроз безопасности в отношении компьютерных систем; оценки соответствия механизмов безопасности компьютерной системы требованиям существующих нормативных документов, а также их адекватности существующим рискам; подготовки аналитического отчета по результатам проведенного анализа; формулирования предложений по устранению выявленных уязвимостей. ПК-3 Знать: национальные, межгосударственные и международные стандарты в области защиты информации; национальные стандарты на проведение научно-исследовательских и опытно-конструкторских работ, сертификационных испытаний и создание систем защиты информации; способы организации работ при проведении сертификации программно-аппаратных средств защиты; принципы построения средств криптографической защиты информации; нормативные правовые акты в области защиты информации; руководящие и методические документы уполномоченных федеральных органов исполнительной власти по
--	---

	защите информации; организационные меры по защите информации. Уметь: анализировать компьютерную систему с целью определения уровня защищенности и доверия; использовать профили защиты и задания по безопасности; применять инструментальные средства проведения сертификационных испытаний; составлять и оформлять аналитический отчет по проведенным сертификационным испытаниям; делать выводы по оценке защищенности на основании аналитического отчета. Владеть: навыками проведения теоретических исследований уровней защищенности компьютерных систем и сетей; проведения экспериментальных исследований уровней защищенности компьютерных систем и сетей; проведения сертификационных испытаний с использованием инструментальных средств; подготовки аналитического отчета по результатам проведенных сертификационных испытаний; формулирования выводов по оценке защищенности.
Трудоемкость, з.е.	4
Форма отчетности	Зачет с оценкой, семестр 10
Перечень основной и дополнительной литературы, необходимой для освоения дисциплины	
Основная литература	1. Девянин, П. Н. Модели безопасности компьютерных систем: [учеб. пособие] / П.Н. Девянин. – М.: Академия, 2005. – 144 с.: ил. – (Высшее профессиональное образование). – На учебнике гриф: Доп.УМО. - Библиогр.: с. 139-140. – ISBN 5-7695-2053-1, экземпляров 1 2. Милославская, Н. Г. Проверка и оценка деятельности по управлению информационной безопасностью: учеб. пособие / Н. Г. Милославская, М. Ю. Сенаторов, А. И. Толстой. – 2-е изд., испр. – М.: Горячая линия-Телеком, 2014. – 166 с.: ил. - (Вопросы управления информационной безопасностью, Кн. 5). - Гриф: Доп. УМО. – Библиогр.: с. 161-163. – ISBN 978-5-9912-0365-4, экземпляров 13
Дополнительная литература	1. Дубинин, Е. А. Оценка относительного ущерба безопасности информационной системы: монография / Е А. Дубинин, Ф. Б. Тебуева, В. В. Копытов. – М.: РИОР: ИНФРА-М, 2014. – 192 с.: табл. – (Научная мысль). – ISBN 978-5-369-01371-7. – ISBN 978-5-16-010120-0, экземпляров 2 2. Мониторинг и аудит информационной безопасности: учеб.-метод. пособие: специальность 090103 – Организация и технология защиты информации / сост. Д. В. Якушев; М-во образования и науки Рос. Федерации, ФГБОУ ВПО "Ставроп. гос. ун-т". – Ставрополь: Изд-во СГУ, 2011. – 69 с. - Библиогр.: с. 66-67, экземпляров 88 3. Оценка защищенности: учеб. пособие / Д. А. Полянский; Владим. гос. ун-т. – Владимир: Изд-во Владим. гос. ун-та, 2005. – 80 с. (Комплексная защита объектов информатизации. Кн. 10 / под. ред. М. Ю. Монахова).